Configure a Content Security Policy (CSP)

Content updated: 09/03/2026

This article is designated for administrators.

About

A **Content Security Policy (CSP)** helps protect your site by controlling which sources the browser can load content from. You can set one up for Content Hubs, legacy Video Portal, and Kaltura Application Framework (KAF) integrations, such as LMS integrations and other third-party integrations.

You can generate a suggested policy, test it without blocking anything, and then apply it. If you use more than one of these, such as Content Hubs and an LMS integration, each one has its own Configuration Management console, so configure a policy in each.

What is a Content Security Policy (CSP)?

A Content Security Policy (CSP) is a list of rules that your site sends to the browser. The rules tell the browser which sources it can load content from, such as scripts, images, styles, fonts, media, and embedded content. The browser blocks anything the policy doesn't allow.

This helps protect your site and its users. Depending on how the policy is set up, it can stop many harmful scripts from running, such as a script that an attacker manages to add to a page. A CSP adds a layer of protection. It doesn't replace other security measures.

For more information about CSP, see Content Security Policy (CSP) on the MDN Web Docs website.

A CSP applies only to pages on your site. It doesn't affect Kaltura media embedded on other websites with a standard embed code.

Kaltura CSP security alert

When you log in to the Configuration Management console, you might see a message recommending that you configure a Content Security Policy (CSP) header for your site.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



This recommendation helps meet standard security requirements. It doesn't mean there's been a security breach.

You can dismiss the message for the current session. It appears again the next time you log in until you configure a CSP.

To configure a CSP, see the steps below.

How to configure a CSP

Overview of the process

Configuration involves three main steps:

1. **Generate** a suggested policy based on your site's configuration.
2. **Test** the policy without blocking content or features, and add any missing sources. Repeat until no unexpected messages appear.
3. **Apply** the tested policy.

Before you begin

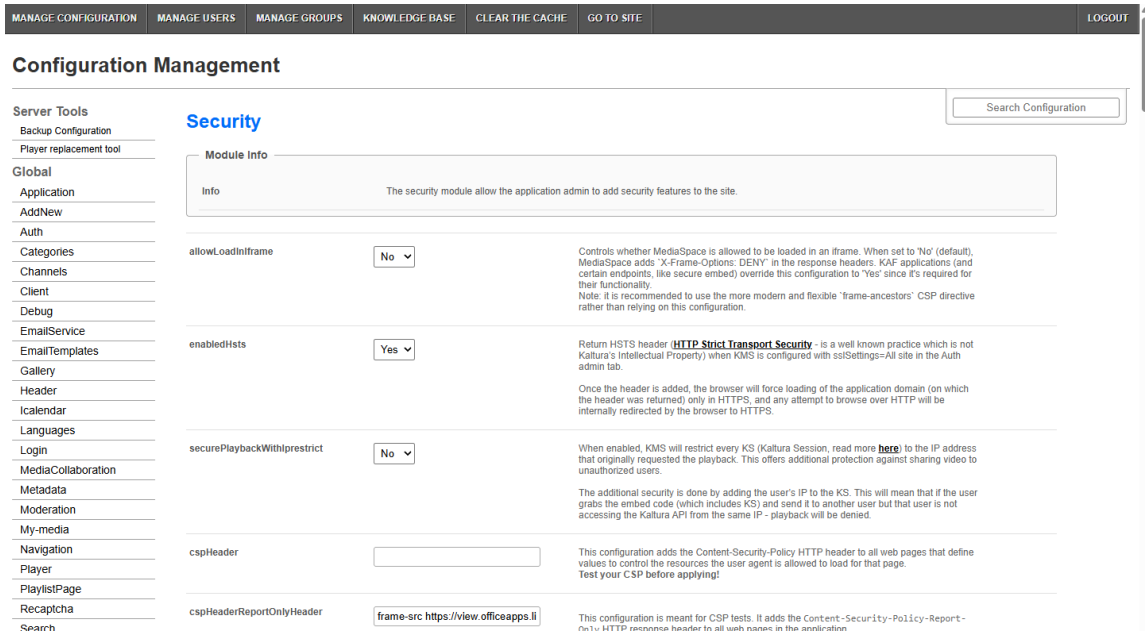
- Use a desktop browser with **developer tools**, such as Google Chrome or Microsoft Edge.
- Have a text editor, such as **Notepad**, to edit the policy.
- Note anything on your site that comes from outside Kaltura, such as a custom logo, design, or fonts, custom code in your site's header or footer, YouTube entries, and third-party integrations. The generated policy covers Kaltura content, so these are the items most likely to need testing in **Step 2**.

Step 1: Generate a suggested policy

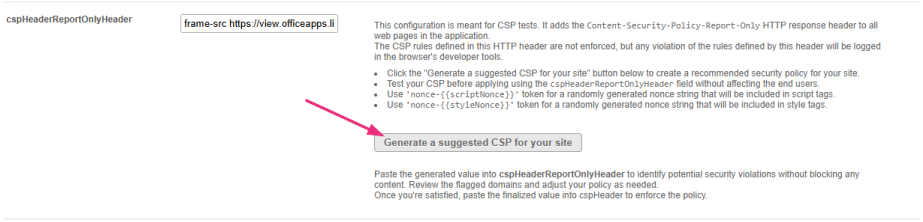
Kaltura generates a suggested policy based on your site's configuration, including the modules that are enabled. Because every site is configured differently, your policy might look different from other sites' policies.

1. Go to your Configuration Management console, and locate the **Security** module.

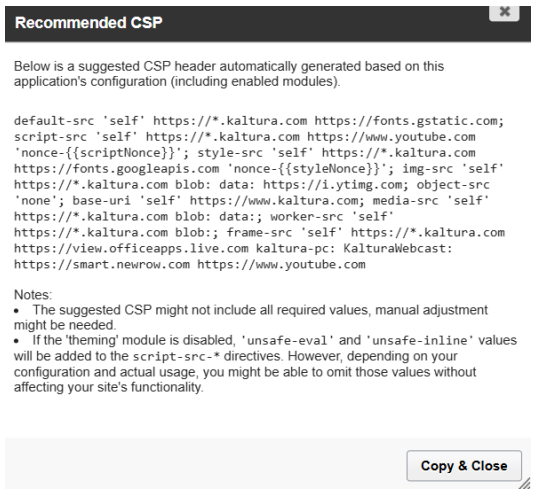
Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



2. Scroll down to the `cspHeaderReportOnlyHeader` field, and select **Generate a suggested CSP for your site**.



The **Recommended CSP** window opens and displays a suggested policy.



3. Select **Copy & Close**, paste the policy into a text editor, such as Notepad, and save the file.

   The policy isn't applied yet. You'll edit this copy while you test the policy.

What the generated policy includes

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

The generated policy includes the sources Kaltura knows are needed, based on your site's configuration and enabled modules. It might still leave out sources that some features need, especially sources that are specific to your site, such as:

- Logos, images, stylesheets, fonts, or scripts hosted on your organization's own domains
- Custom modules and third-party integrations
- Custom JavaScript added to your site's header or footer
- Media delivered through remote storage, a custom delivery profile, or an enterprise content delivery network (eCDN)

You'll find any missing sources when you test the policy in **Step 2**.

The generated policy also depends on whether Theming is enabled on your site:

- **If Theming is enabled** on your site, the policy uses nonce tokens instead of `'unsafe-inline'` and `'unsafe-eval'`. For more information about nonce tokens, see Content Security Policy (CSP) directives and sources. Even if Theming is enabled on your site, some pages, such as the media page or the editor, might not use Theming. These pages might need different values. If you see messages that start with *Applying inline style* or *Executing inline script* when you test these pages, contact Kaltura Support.
- **If Theming isn't enabled** on your site, the policy includes `'unsafe-inline'` in the `script-src` and `style-src` directives, and `'unsafe-eval'` in `script-src`. Pages that don't use Theming need these values to work. These values reduce the protection the policy gives, so we recommend enabling Theming on your site. Don't remove these values unless Kaltura Support or your security team confirms that your site doesn't need them.

Test the generated policy in the `cspHeaderReportOnlyHeader` field before you apply it in `cspHeader`. The report-only policy lets you review potential violations without affecting end users.

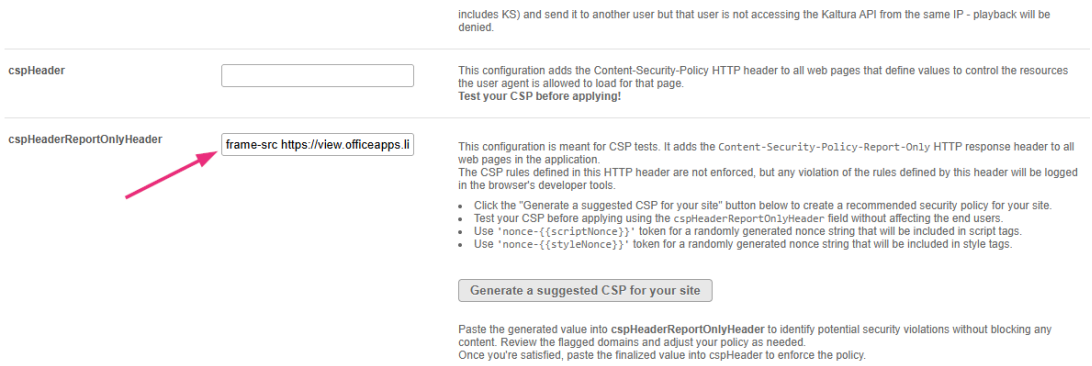
Step 2: Test the policy

Test your policy by adding it to the `cspHeaderReportOnlyHeader` field. This puts the policy in **report-only** mode. The browser reports potential violations, but doesn't block any resources. This way, you can find and fix problems before they affect your users.

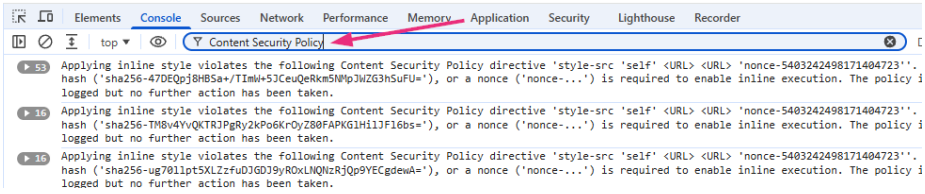
Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

Set up the browser Console

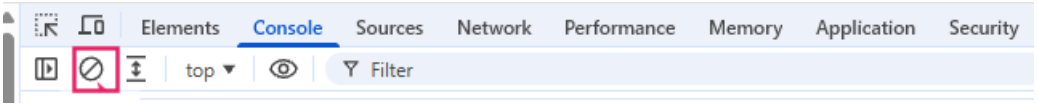
1. In the **Security** module, paste the policy you copied in Step 1 into the **cspHeaderReportOnlyHeader** field. Paste only the policy. Don't include the `Content-Security-Policy:` header name.



2. Select **Save**.
   The policy is active in report-only mode.
3. Open your site in a new browser tab. For a KAF integration, open a page in the third-party application that shows Kaltura content, such as My Media in your LMS.
4. From that tab, open your browser's developer tools (press **F12**, or on a Mac, press **Cmd + Option + J**), and select the **Console** tab.
   The Console lists the resources that the policy would block.
5. In the **Filter** box, type `Content Security Policy`.
   Messages about the Content Security Policy appear. The Console also shows many messages that aren't about CSP, and the filter hides most of them.



6. Select the **Console settings** (gear) icon, and select **Keep log**. In some browsers, this option is called **Preserve log**.
   Normally, the Console clears its messages each time a new page loads. With this option selected, messages from every page you visit stay in the list, so you don't miss a problem on a page you've already left.
7. Select the **Clear** icon to remove existing messages, so you only see results from this test.



Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

8. Refresh the page.
   The page loads with the policy you just saved.

Test your site's features

1. In the same browser tab, open your site's main pages, such as the home page and a media page, and play a video. Then try each item on your list.
   The Console only shows messages for the tab it's open in. The browser loads a resource only when you use the feature that needs it. For example, the YouTube player script loads only when you play a YouTube entry.
2. After each action, check the Console for new messages.
   If the policy would block a resource, a message appears. The message ends with *The policy is report-only*, which confirms that the resource was reported but not blocked. In report-only mode, CSP messages aren't shown in red, because nothing is blocked. Use the filter to find them.

If you see CSP messages, see Troubleshoot Content Security Policy (CSP) messages in the browser Console. Repeat the test until no unexpected messages appear, and then continue to **Step 3**.

Step 3: Apply the tested policy

When you add the tested policy to `cspHeader`, the browser blocks resources that the policy doesn't allow.

Before you apply the policy, back up your site configuration. If the applied policy causes problems, you can restore the backup. For more information, see Backup and restore configuration data in Content Hubs and legacy Video Portal.

Don't select Save until you've completed all the field changes below. This prevents the site from being left in a partially configured state.

1. Copy the tested policy from your text editor.
2. Paste it into the **cspHeader** field.
3. Clear the **cspHeaderReportOnlyHeader** field.
4. Select **Save**.
   The policy is applied. The browser now blocks resources that the policy doesn't allow.
5. Test the site's main features again, with the browser Console open.
   If you missed a feature while testing, this is where you'll find out. If a resource is

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

blocked, a red message ending with *The action has been blocked* appears. Add the missing source as described in Troubleshoot Content Security Policy (CSP) messages in the browser Console.

After `cspHeader` contains a policy, the CSP security alert no longer displays when administrators log in to the Configuration Management console.

Do I need a separate policy for the Configuration Management console?

In most cases, you don't need a separate policy. When `adminCspHeader` is empty, the Configuration Management console uses the policy in the `cspHeader` field.

Configure a separate policy only when the console needs to load different content or connect to different sources from your site. Use the following fields:

- `adminCspHeaderReportOnlyHeader` - Tests a separate policy for the console without blocking content or features.
- `adminCspHeader` - Applies the tested policy to the console instead of the policy in `cspHeader`.

Before you make any changes to `adminCspHeader`, back up your site configuration. For more information, see Backup and restore configuration data in Content Hubs and legacy Video Portal. Then test the policy in `adminCspHeaderReportOnlyHeader` before applying it. If a console policy blocks access to the Configuration Management console, you can't restore the backup yourself. Contact Kaltura Support.

Troubleshooting

Issue	What to do
No policy is generated.	This usually means your site has a unique configuration. Don't enter or apply an empty policy. Contact Kaltura Support so they can review your site's settings.
A feature stops working after you apply the policy.	Open the browser Console and look for red messages ending with *The action has been blocked*. Add the missing source to the policy in the `cspHeader` field.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

Issue	What to do
You can't access the Configuration Management console after applying a policy.	Contact Kaltura Support.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.